PhishMe Simulator™

SZKOLENIE PRACOWNIKÓW DOTYCZĄCE ODPORNOŚCI NA PHISHING

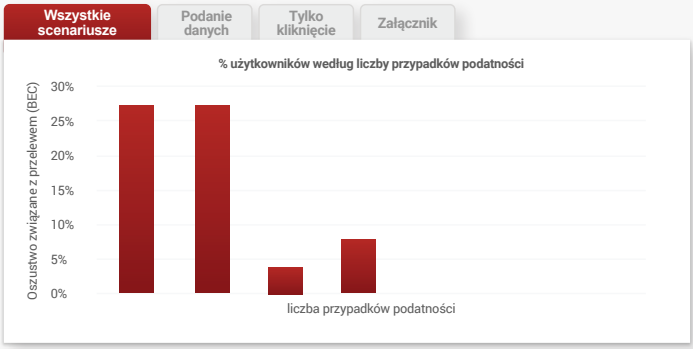
Badania PhishMe Research wykazały, że ataki ransomware stanowiły ponad 97% phishingowych wiadomości e-mail wysłanych w 2016 roku. Przy tak alarmujących liczbach, jak można zapobiec atakom na firmę? PhishMe Simulator zmienia pracowników w ostatnią linię obrony, wykorzystując sprawdzone metody szkolenia behawioralnego, aby lepiej przygotować pracowników do rozpoznawania szkodliwych ataków i zapobieganiu im, przekształcając najbardziej podatny element w najważniejszy element obrony przed atakami.

Dlaczego należy wybrać PhishMe Simulator™?

Udowodniono, że program PhishMe zmniejsza ryzyko związane z zaawansowanymi atakami cybernetycznymi ukierunkowanymi na pracowników o nawet 95% – to Twoja ostateczna broń przeciwko niebezpiecznym próbom phishingu.

Najważniejsze korzyści

- ✓ Zmniejsza podatność organizacji na ataki typu phishing o ponad 95% dzięki odpowiednim szkoleniom
- ✓ Symuluje najnowsze taktyki przeprowadzania ataków z wykorzystaniem edytowalnych scenariuszy i szablonów
- ✓ Stosuje zróżnicowane techniki szkoleniowe znajdujące się w bibliotece materiałów w wielu językach
- ✓ Ocenia wydajność programu i identyfikuje zagrożone obszary przy użyciu szczegółowych raportów

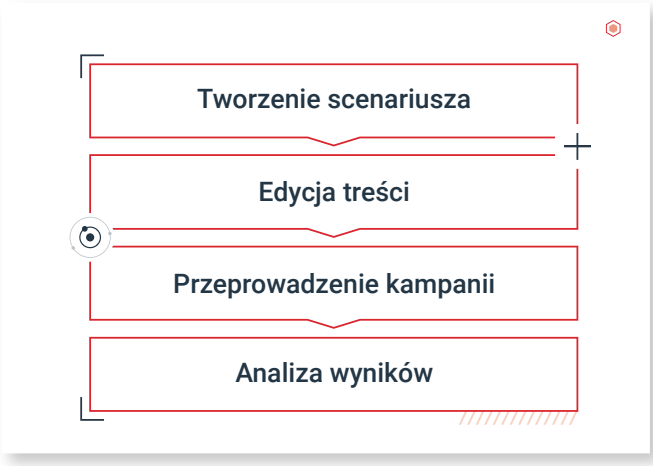


Czym jest PhishMe Simulator™?

Simulator to **specjalna platforma SaaS**, która poprawia reakcje pracowników na ataki i ułatwia im dostarczanie informacji na temat zagrożeń w czasie rzeczywistym poprzez symulowanie prawdziwych ataków typu spear-phishing. Edytowalne scenariusze symulują najczęściej występujące zagrożenia i dostarczają informacje zwrotne i dane osobom, które padły ofiarą tego typu ataków.

Nasza opatentowana technologia zapewnia niezrównany wachlarz schematów cyber-ataków, treści na ich temat oraz możliwości dostosowywania. Dla każdego scenariusza przygotowywana jest szczegółowa analiza i raport. Światowej jakości obsługa klienta PhishMe zapewnia, że ćwiczenia przeprowadzane są w sposób kontrolowany, który nie ma negatywnego wpływu na bezpieczeństwo organizacji.

Sposób działania



> Usprawnione raporty analizy PhishMe są nieocenione. Dzięki tym danym byliśmy w stanie zmodyfikować nasze programy obrony przed phishingiem poprzez odpowiednie szkolenia. Skupiliśmy się szczególnie na ograniczeniu liczby pracowników, którzy często otwierają otrzymane łącza i załączniki.
>
> **Jim Stewart, CISO, United Community Bank**

Dostosowywana treść i odpowiednie szkolenia

Scenariusze symulatora można dostosować tak, aby symulowały wiele różnych technik, w tym ataki typu „drive-by", złośliwe oprogramowanie oraz ataki wykorzystujące inżynierię społeczną, jak również bardziej zaawansowane ataki, jak np. wyłudzanie informacji podczas rozmowy oraz spersonalizowane ataki typu spear phishing. Dodatkowo klienci mogą wdrażać scenariusze, które pozwalają sprawdzić postępy w porównaniu z rosnącą liczbą klientów PhishMe.

Klienci mogą tworzyć swoje własne scenariusze lub użyć jednego z dziesiątek dostępnych szablonów. Nasza rosnąca biblioteka treści obejmuje wiele tematów związanych z phishingiem, świadomością znaczenia bezpieczeństwa, zgodności i mediów społecznościowych w wielu różnych formatach, m.in. szablony HTML 5, filmy i moduł gier. Dzięki materiałom dostępnym w wielu językach PhishMe spełnia potrzeby lokalnych i globalnych organizacji.

Organizacjom, które wymagają kompleksowego szkolenia, PhishMe oferuje w pełni zgodne ze SCORM materiały na temat ogólnych zagadnień w kwestii bezpieczeństwa. **Dostępne szkolenia obejmują następujące zagadnienia:**

- Świadomość zagrożenia atakami typu spear phishing
- Złośliwe łącza
- Złośliwe oprogramowanie
- Bezpieczne hasła
- Ochrona danych
- Urządzenia przenośne
- Bezpieczne przeglądanie sieci
- Inżynieria społeczna
- Portale społecznościowe
- Bezpieczeństwo fizyczne
- Praca poza biurem
- Zgłaszanie podejrzanych sytuacji
- Oprogramowanie typu ransomware
- Naruszenie bezpieczeństwa firmowej poczty elektronicznej (Business Email Compromise, BEC)
- Zaawansowane ataki typu spear phishing

Bezpieczna platforma

Nasza platforma SaaS znajduje się w placówce posiadającej certyfikaty SOC 2 i SOC 3 Tier III w Stanach Zjednoczonych oraz w placówce zgodnej z ISO9001:2008 w Europie. Obie placówki są regularnie poddawane testom penetracyjnym i wyposażone są w rozbudowane funkcje kontroli dostępu. Wszystkie dane są szyfrowane, a PhishMe nigdy nie gromadzi danych klientów podczas scenariuszy podawania danych.

Szczegółowa analiza

Każdy scenariusz umożliwia analizę wielu danych, które analizowane w dłuższym okresie pozwalają poznać słabe punkty organizacji i opracować plan rozwoju i usprawnień.

Symulator śledzi między innymi:

- Geolokalizację
- Znaczniki czasu
- Indywidualne odpowiedzi
- Tendencje
- Czas poświęcony szkoleniu
- Czas do pierwszego zgłoszenia (wymagana funkcja Reporter)
- Listę przeglądarek
- Odporność organizacji (wymagana funkcja Reporter)

Gwarancja sukcesu

Każda licencja Simulator obejmuje dostęp do światowej klasy wsparcia PhishMe. Poza gwarancją poprawnego dostarczania scenariuszy opartych na wiadomościach e-mail, nasz zespół wsparcia oferuje porady dotyczące wdrażania usługi Simulator, porównywania scenariuszy z najlepszymi praktykami, dostosowywania programu do kultury, kierownictwa i użytkowników w organizacji oraz wspomaga wdrażanie nowych funkcji i scenariuszy.

W przypadku ograniczonych zasobów organizacje mogą wykorzystać usługę Simulator jako częściowo lub w pełni zarządzane rozwiązanie korzystające z usług oddelegowanego eksperta, który tworzy, wdraża i analizuje kampanie. Programy dostosowane są do wymagań i kultury organizacji.

PhishMe jest wiodącym dostawcą rozwiązań obrony przed phishingiem dla organizacji obawiających się najpopularniejszego obecnie rodzaju ataku — spear phishing. Opierająca się na informacjach platforma PhishMe zamienia pracowników w aktywną linię obrony, umożliwiając im identyfikowanie, zgłaszanie i zapobieganie atakom typu spear phishing i „drive-by" oraz wykorzystującym złośliwe oprogramowanie. Nasze otwarte podejście umożliwia łatwą integrację PhishMe z systemami zabezpieczeń, co zapewnia widoczne usprawnienie procesu decyzyjnego organizacji w kwestii bezpieczeństwa. Klienci PhishMe należą do przemysłów obronnego, produkcyjnego i energetycznego, branży usług finansowych oraz opieki zdrowotnej. Poza tym, naszymi klientami jest 1000 globalnych organizacji, które zrozumiały, że zmiana zachowań użytkowników pozwoli poprawić bezpieczeństwo i reakcje na wydarzenia oraz zmniejszyć ryzyko narażenia.

PHISHME

30-dniowy darmowy okres próbny

Rozpocznij budowę najlepszego systemu ochrony przed phishingiem wykorzystującego pracowników.

Więcej informacji znajduje się na stronie www.phishme.com